DE SAN BERNARDO[1] A REDMON[2] PASANDO POR LANGLEY[3]: HISTORIA DE UN VIAJE SIN CONTROL

From St. Bernard to Redmon via Langley: a story of uncontrolled travel

Por Fernando Javier Cremades López de Teruel
Doctorando en Derecho por la Universidad Pablo de Olavide de Sevilla
Letrado de la Administración de Justicia
cremades_ferlop@gva.es

Artículo recibido: 15/04/23 | Artículo aceptado: 19/06/23

RESUMEN

Anuladas por el TJUE las Decisiones de la Comisión europea llamadas "Puerto seguro" y "Escudo de la privacidad", los Estados miembros de la UE empiezan a desaconsejar, sino a prohibir, el uso en sus centros educativos, administración es públicas y programas de salud pública la suite ofimática Office 365 por incumplir las exigencias del Reglamento General de Protección de Datos (UE), permitir a Microsoft el acceso a datos personales de los usuarios, transferirlos a EE.UU., y posibilitar a las agencias de inteligencia estadounidenses el acceso a los mismos. Mientras, el sistema judicial español, sin control, vigilancia ni advertencia alguna, se lanza en brazos de Microsoft y de su línea de productos. Este trabajo es una guía del viaje que hacen los datos personales que son tratados en los juzgados y tribunales españoles a la sede del FBI en EE.UU.

ABSTRACT

Annuls by the Court of Justice of the European Union the Decisions of the European Commission called "Safe Harbor" and "Privacy Shield", the EU Member States begin to discourage, if not to prohibit, the use in their educational centers, public administrations and public health programs the office suite Office 365 for failing to comply with the requirements of the General Data Protection Regulation (EU), allowing Microsoft access to users' personal data, transfer them to the U.S., and enable U.S. intelligence agencies to access them. Meanwhile, the Spanish judicial system, without any control, surveillance or warning, it is launched into the arms of Microsoft and its product line. This work is a guide to the journey made by personal data that are processed in the Spanish courts and tribunals to the headquarters of the FBI in the USA.

[1] Calle San Bernardo 45, 28015, Madrid. Sede del Ministerio de Justicia de España.
[2] Redmond, Washington, Estados Unidos. Sede corporativa de Microsoft.
[3] Langlay, Virginia, Estados Unidos. Oficinas centrales de la CIA.

PALABRAS CLAVE

Datos, Judicial, Microsoft, Transferencia, Schrems, Control, Puerto, Escudo, Infracción, Estado, Facebook, Google, Office 365.

KEYWORDS

Data, Judicial, Microsoft, Transfer, Schrems, Control, Port, Shield, Infringement, Status, Facebook, Google, Office 365.

Sumario: 1. Maximiliam Schrems. 2. La Decisión *Safe Harbor* o puerto seguro. 3. Schrems I. 4. Schrems II. 5. ¿Y tras Schrems I y Schrems II?. 6. Hablemos del sistema judicial español. 7. Y, finalmente, las claves de este viaje (y sus coordenadas). 8. Bibliografía.

Dedicado a Sonia, Alfredo y Jesús,
porque la medida del estímulo no es el número sino la intensidad.

1. Maximiliam Schrems

Este relato principia con Maximiliam Schrems, un estudiante austríaco usuario de la red social Facebook. Maximiliam presentó el 25 de junio de 2013 una reclamación ante la autoridad de control irlandesa en materia de protección de datos de carácter personal por la que solicitaba que se prohibiese a Facebook Ireland la transferencia de sus datos personales a servidores pertenecientes a Facebook Inc. ubicados en territorio de los Estados Unidos de América (en adelante, EE.UU.).

El Reglamento General de protección de Datos (en adelante, RGPD)[4] dedica sus artículos 44 a 50 a la transferencia de datos personales a terceros países u organizaciones internacionales. De su contenido podemos extraer las siguientes conclusiones:

1) la transferencia de datos de carácter personal a un país tercero solo puede llevarse a cabo, en principio, si el país tercero en cuestión garantiza un nivel de protección adecuado a dichos datos[5];

[4] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[5] Artículo 44 del RGPD: "Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado."

2) se podrá realizar una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión Europea haga constar que un país tercero, a la vista de su legislación interna o de sus compromisos internacionales, garantiza un nivel de protección adecuado[6];
3) a falta de esta decisión de adecuación, la transferencia de datos solo podrá realizarse si el exportador de datos personales, establecido en la Unión Europea (en adelante, UE), ofrece garantías adecuadas, que pueden derivar de cláusulas tipo de protección de datos adoptadas por la Comisión, y si los interesados cuentan con derechos exigibles y acciones legales efectivas[7]; y
4) en este caso de ausencia de una decisión de adecuación o de garantías adecuadas, la transferencia de datos únicamente se realizará si se cumple alguna de las condiciones siguientes[8]:

a) el interesado ha dado explícitamente su consentimiento a la transferencia propuesta;
b) la transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento, o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;
c) la transferencia es necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;
d) la transferencia es necesaria por razones importantes de interés público;

---

[6] Artículo 45.1 del RGPD: "Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica."

Artículo 45.3 del RGPD: "La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2."

[7] Artículo 46.1 del RGPD: "A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas."

Artículo 46.2, letra c), del RGPD: "cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2; (…)"

[8] Artículo 49.1 del RGPD.

e) la transferencia es necesaria para la formulación, el ejercicio o la defensa de reclamaciones;
f) la transferencia es necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;
g) la transferencia se realiza desde un registro público que tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo.

Para el caso de que una transferencia no pueda basarse en una decisión de adecuación o de las garantías adecuadas, y tampoco le resulten aplicables las excepciones a que hemos hecho referencia, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evalúa todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofrece garantías apropiadas con respecto a la protección de datos personales.

Como sabemos el modelo regulatorio que acoge la UE en materia de protección de datos de carácter personal es horizontal, esto es, una norma general que afecta a todos los órdenes, ámbitos y actividades. Al tiempo de los acontecimientos que estamos relatando, era la Directiva 95/46 y, en la actualidad, es el RGPD.

Sin embargo, otros países adoptan otro tipo de planteamientos normativos y éstos se deben sujetar a los requisitos de adecuación que la normativa de la UE exige para que se les puedan transferir datos.

Uno de estos países es EE.UU. Si bien cuenta con una serie de regulaciones sectoriales en la materia -es más, algunos de sus Estados han dictado normas sobre privacidad-, carece formalmente de una norma federal que sea de aplicación general y uniforme. Esto determinó la necesidad de convenir un punto de encuentro para posibilitar las transferencias de datos de la UE a aquel país salvando las restricciones que para estos casos imponía la Directiva 95/46.

El primero de estos puntos de encuentro fue lo que se vino a llamar *Safe Harbor* o principios de puerto seguro, un sistema de autorregulación adoptado por el Departamento de Comercio de EE.UU. al que se podían adherir las empresas en ese país bajo el compromiso de cumplir las reglas consignadas en su texto. En el año 2000 la Comisión Europea declaró adecuado este sistema dando lugar a la Decisión 2000/520.

Retornando a Maximiliam Schrems, como todo usuario de la red social Facebook residente en el territorio de la UE, en el momento de su inscripción a este servicio está obligado a aceptar un contrato con Facebook Ireland, filial de

Facebook Inc., domiciliada ésta última en EE.UU., en cuya virtud sus datos personales se transfieren, en todo o en parte, a servidores pertenecientes a Facebook Inc, situados en el territorio de EE.UU., donde son objeto de tratamiento.

Por tal razón, Schrems reclamó a la autoridad de control irlandesa que, en cumplimiento de sus competencias, prohibiese a Facebook Ireland transferir sus datos personales a EE.UU. Para ello alegó que el Derecho y las prácticas de los EE.UU. no ofrecían suficiente protección frente al acceso a los datos transferidos a ese país por parte de sus autoridades públicas. Es más, afirmó la inquietud que habían generado las revelaciones de Edward Snowden[9] sobre las actividades de los servicios de información de aquel país, en particular las de la Agencia Nacional de Seguridad[10].

La autoridad de control le respondió que nada podía hacer dado que Facebook, al igual que otras relevantes compañías estadounidenses, estaba adherida a la llamada Decisión *Safe Harbor*.

2. La Decisión *Safe Harbor* o puerto seguro

En un momento álgido de la preocupación por la protección de los datos de carácter personal y el desarrollo tecnológico asociado al tratamiento masivo de los datos, las diferencias normativas entre la UE y los EE.UU. eran tan grandes que la legislación europea impedía transferir datos a estos últimos al no contar con unas determinadas exigencias de seguridad.

Esto llevó en el año 2000 a que la Comisión Europea y las autoridades norteamericanas alcanzaran un acuerdo que dotase de un mínimo de seguridad jurídica a la transmisión internacional de datos. Este acuerdo fue la Decisión 2000/520 de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes publicadas por el Departamento de Comercio de Estados Unidos de América[11]. Con esta Decisión la Comisión venía a declarar que los principios de puerto seguro garantizaban un nivel adecuado de protección de los datos personales transferidos desde la UE a entidades establecidas en los EE.UU.

[9] Edward Joseph Snowden (Elizabeth City, Carolina del Norte; 21 de junio de 1983) es un consultor tecnológico estadounidense y naturalizado ruso, ex empleado de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA). En junio de 2013, a través de los periódicos *The Guardian* y *The Washington Post*, Snowden hizo públicos documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y XKeyscore. https://es.wikipedia.org/wiki/Edward_Snowden

[10] Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015. Asunto C-362/14.

[11] DO 2000, L 215, p. 7

La calificación "puerto seguro" era concedida por la Comisión europea, proporcionaba al favorecido una presunción de cumplimiento de una serie de principios para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos, y le dispensaba de la obligación de tener que cumplir cada uno de los requisitos particulares impuestos por el Estado nacional de la persona titular de los datos afectados.

Los criterios evaluados por la Comisión para conceder esta calificación iban desde la existencia de medios de información para los afectados, la posibilidad de oposición de éstos, la seguridad e integridad de los datos, y hasta los medios de acceso o la posibilidad de satisfacción de los derechos de los interesados.

A este acuerdo se adhirieron, además de Facebook, compañías como Google, Amazon y Apple, lo que les permitió su reconocimiento como puertos seguros y, en consecuencia, establecer un tráfico fluido de datos entre la UE y los EE.UU. Este acuerdo no significó un reconocimiento de seguridad para toda la nación sino, exclusivamente, para aquellas empresas que por aplicar las buenas prácticas establecidas por el organismo regulador les permitía obtener su reconocimiento como puerto seguro.

En definitiva, dado que Facebook tenía reconocida la condición de puerto seguro y se debía presumir un tratamiento de datos adecuado a las garantías exigidas por la Unión Europea, la autoridad de control irlandesa desestimó la reclamación.

Frente a esta decisión, Schrems presentó una reclamación ante el Tribunal Supremo irlandés que, a su vez, el 25 de julio de 2014, elevó una cuestión prejudicial al Tribunal de Justicia de la Unión Europea acerca de las garantías que ofrecía Facebook en relación con el tratamiento de sus datos personales, y sobre el cumplimiento de las obligaciones y garantías que impone la legislación europea para que se pueda autorizar una trasferencia de datos a EE.UU.[12].

[12] Petición de decisión prejudicial planteada por la High Court of Ireland (Irlanda) el 25 de julio de 2014—Maximillian Schrems/Data Protection Commissioner (Asunto C-362/14) (2014/C 351/06). Órgano jurisdiccional remitente High Court of Ireland Partes en el procedimiento principal. Demandante: Maximillian Schrems. Demandada: Data Protection Commissioner. Cuestiones prejudiciales:

1) En el marco de la resolución de una reclamación presentada ante una autoridad independiente a la que la ley ha conferido las funciones de aplicar y ejecutar la legislación en materia de protección de datos, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, los Estados Unidos de América) cuya legislación y práctica no prevén supuestamente una protección adecuada de la persona sobre la que versan los datos, ¿está vinculada dicha autoridad en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión de la Comisión de 26 de julio de 2000 (2000/520/CE), habida cuenta de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01), no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE? 2) O bien, con carácter subsidiario, ¿puede y/o debe realizar el titular del cargo su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión de la Comisión? Asunto C-362/14: Petición de decisión prejudicial planteada por la

El tribunal si bien reconoció que la vigilancia electrónica y la interceptación de los datos personales transferidos desde la UE a EE.UU. servían a finalidades necesarias e indispensables para el interés público, no podía eludir que las revelaciones de Snowden habían demostrado que la Agencia Nacional de Seguridad (NSA) de los EE.UU., así como otros organismos federales, como el Federal Bureau of Investigation (FBI), habían cometido importantes excesos.

3. Schrems I

Hemos visto que el funcionamiento de la Decisión 2000/520 se basa, por un lado, en los compromisos y la autocertificación de las entidades que la han suscrito y, por otro, en su adhesión voluntaria y sus reglas vinculantes para los que los suscriben[13].

Sin embargo, la aplicación de esta Decisión estuvo desde un primer momento sometida a un seguimiento que pronto empezó a arrojar conclusiones inquietantes que aconsejaban su revisión. Así, el 27 de noviembre de 2013 la Comisión adoptó la Comunicación al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE[14], que plasmó las siguientes conclusiones:

> 1) la cada vez más extendida existencia en los Estados Unidos de programas de vigilancia que comprendían la recogida y el tratamiento de datos personales a gran escala;
>
> 2) una creciente preocupación por el nivel de protección de los datos personales de los ciudadanos de la UE transferidos a EE.UU. en el marco del régimen de puerto seguro;
>
> 3) la mayoría de las empresas estadounidenses más directamente relacionadas con los programas de vigilancia están certificadas en el marco del régimen de puerto seguro que se ha convertido en uno de los conductos a través de los cuales se da acceso a las autoridades de inteligencia estadounidenses para recopilar datos personales que proceden de la UE;
>
> 4) las autoridades estadounidenses pueden tratar los datos personales de los ciudadanos de la UE enviados a EE.UU. en el marco del régimen de puerto seguro más allá de lo estrictamente necesario para la protección de la seguridad nacional, y de forma incompatible con los motivos por los

High Court of Ireland (Irlanda) el 25 de julio de 2014 — Maximillian Schrems/Data Protection Commissioner (europa.eu).

[13] Artículo 1 de la Decisión de la Comisión de 26 de julio de 2000. 2000/520/CE

[14] Comunicación al Parlamento Europeo y al Consejo titulada «Restablecer la confianza en los flujos de datos entre la UE y EE.UU.» [COM(2013) 846 final; en lo sucesivo, «Comunicación COM(2013) 846 final»]

que se recogieron inicialmente dichos datos en la Unión y con los fines por los que se transfirieron a EE.UU.;

5) las empresas estadounidenses certificadas no respetan los principios de puerto seguro, o no lo hacen plenamente.

6) las garantías previstas por la legislación estadounidense se refieren fundamentalmente a los ciudadanos estadounidenses, o a los residentes legales, no estando prevista la posibilidad de que los titulares de los datos, ya sean estadounidenses o de la UE, puedan acceder a sus datos, rectificarlos o suprimirlos, ni obtener reparación administrativa o judicial, en lo que respecta a la recogida y el tratamiento posterior de sus datos personales en virtud de los programas de vigilancia estadounidenses.

La Comisión concluía su Comunicación afirmando la necesidad urgente de debatir con las autoridades de EE.UU. las deficiencias detectadas para poder seguir manteniendo la aplicación del régimen de puerto seguro.

El clima de desconfianza era creciente, especialmente desde las revelaciones que realizó un excontratista de la NSA y la CIA, Edward J. Snowden, quien a través de la filtración de miles de documentos clasificados de alto secreto puso de manifiesto un sistema gubernamental de espionaje masivo de las telecomunicaciones globales. Los informes publicados en distintos medios de comunicación acreditaron la existencia una red de colaboración entre distintas agencias de inteligencia para una transferencia masiva de metadatos, registros y otras informaciones a la Agencia de Seguridad Nacional (NSA) de EE.UU.

El propio tribunal irlandés a la hora de plantear la cuestión prejudicial llegó a cuestionar la aplicabilidad de la Decisión puerto seguro a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea[15] así como de los principios enunciados por el Tribunal de Justicia en la sentencia Digital Rights Ireland y otros (C-293/12 y C-594/12). Afirmó el tribunal que el derecho al respeto de la vida privada garantizado por el artículo 7 de la Carta y por los valores esenciales comunes a las tradiciones de los Estados miembros quedarían sin contenido si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y generalizada, sin ninguna justificación objetiva y sin que esas prácticas se rodeen de garantías adecuadas y comprobables[16].

[15] "Artículo 7 Respeto de la vida privada y familiar Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. Artículo 8 Protección de datos de carácter personal 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

[16] (34) Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015. Asunto C-362/14.

El tribunal fue más allá y entendió que, en definitiva, lo que pretende impugnar el Sr. Schrems es la propia validez de la Decisión de puerto seguro, de modo que lo que debe decidirse es si ante una denuncia de infracción de la Directiva 95/46[17], por entonces vigente, la autoridad de control nacional está vinculada por la presunción de garantía que atribuye la Decisión, o bien puede cuestionarla e iniciar su propia investigación.

En definitiva, la High Court irlandesa preguntó al Tribunal de Justicia de la Unión Europea si una decisión, como la 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, impide que una autoridad de control de un Estado miembro pueda examinar la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de sus datos personales transferidos desde un Estado miembro a ese tercer país, cuando esa persona afirma que el Derecho y las prácticas en vigor en ese país no garantizan un nivel de protección adecuado[18].

El TJUE respondió lo siguiente:

> a) la normativa europea sobre protección de datos personales prohíbe la transferencia de datos de ciudadanos europeos a un tercer país si éste no ofrece un nivel de protección adecuado[19];
>
> b) por "nivel de protección adecuado" no se debe entender que este tercer país deba garantizar efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la UE por la Directiva 95/46, entendida a la luz de la Carta de los Derechos Fundamentales de la Unión Europea. Basta con que los medios aplicados en ese tercer país, aunque distintos, sean eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión[20];
>
> c) si bien la Comisión europea, a la hora de adoptar la Decisión 2000/520, debió comprobar que legislación aplicable en el tercer país al que se van a transferir los datos personales, así como la práctica empleada para asegurar su cumplimiento, es conforme a la normativa europea aplicable[21], lo cierto es que los principios de

[17] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. (Disposición derogada).

[18] (37) Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015. Asunto C-362/14.

[19] (49) Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015. Asunto C-362/14.

[20] (73) Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015. Asunto C-362/14.

[21] (75) Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015. Asunto C-362/14.

puerto seguro que construyen la Decisión son aplicados, y exigidos, únicamente a las entidades estadounidenses autocertificadas como puerto seguro que reciben datos desde la UE, y sin que estos principios resulten exigibles a las autoridades públicas estadounidenses[22];

d) al reconocer la Decisión 2000/520 una primacía de las exigencias de seguridad nacional, interés público y cumplimiento de la ley de EE.UU. sobre los principios de puerto seguro, se posibilita que las autoridades públicas estadounidenses puedan acceder a los datos personales que reciban de la UE estas empresas autocertificadas, sin límite alguno y sin establecer ninguna diferenciación, limitación o excepción, y sin un control de su utilización posterior a fines concretos y específicos[23];

e) en definitiva, la Decisión 2000/520 en ningún momento manifiesta que los EE.UU. garantizan efectivamente un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales; tan solo establece un sistema de autocertificación y de presunción de adecuación, a través del compromiso de cumplimiento de unos principios de puerto seguro; aplicable exclusivamente a las empresas estadounidenses que reciben, almacenan y someten a tratamiento los datos que reciben de la UE; y no así a las autoridades públicas de los EE.UU. que sin límites ni restricciones, y por entender comprometida la seguridad nacional, el interés público o por exigencias de la ley de EE.UU. pueden acceder sin límites ni restricciones a estos datos y para los fines que consideren convenientes.

En consecuencia, el TJUE "sin que sea preciso apreciar el contenido de los principios de puerto seguro", resuelve "que el artículo 1 de esa Decisión vulnera las exigencias establecidas por el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta, y es inválido por esa causa."[24]

Al tiempo, el TJUE manifiesta que la adopción de una Decisión por la que la Comisión Europea afirme que un tercer país garantiza un nivel de protección adecuado no impide que una autoridad de control de un Estado miembro pueda examinar cualquier solicitud de una persona relativa a la protección de sus derechos y libertades, frente al tratamiento de sus datos personales transferidos

[22] (82) Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015. Asunto C-362/14.

[23] (86, 87 y 93) Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015. Asunto C-362/14.

[24] (98) Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015. Asunto C-362/14.

desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

4. Schrems II

La invalidación de la Decisión 2000/520 por el TJUE determinó la necesidad de acordar un nuevo mecanismo para posibilitar las transferencias internacionales de datos de acuerdo con las exigencias normativas de la UE. Este nuevo instrumento fue la Decisión 2010/87[25], llamada *Privacy Shield*, y que se basaba en el modelo de cláusulas contractuales tipo que introdujo su precedente Decisión 2002/16. Con este mecanismo se pretende posibilitar la transferencia internacional de datos en base a la garantía que debe implicar la incorporación de cláusulas contractuales apropiadas, y que los Estados miembros no debían rechazar como garantías adecuadas al amparo de la Directiva 95/46.

De este modo, la Decisión 2010/87 viene a regular las cláusulas contractuales tipo y se limita a establecer que estas cláusulas pueden ser utilizadas por un responsable del tratamiento de datos establecido en la UE a fin de ofrecer garantías suficientes a los efectos del artículo 26, apartado 2, de la Directiva 95/46/CE para la transferencia de datos personales a un encargado del tratamiento establecido en un tercer país[26].

Las cláusulas contractuales tipo se incluyen en el anexo de la Decisión y, se afirma, ofrecen las garantías adecuadas con respecto a la protección de la vida privada y de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los correspondientes derechos, según exige la Directiva 95/46/CE[27].

Anulada la Decisión 2000/520 y posibilitado que las autoridades de control nacionales puedan examinar cualquier solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de sus datos que se hayan transferido desde un Estado miembro a un tercer país, la autoridad de control irlandesa instó a Maximiliam Schrems a que reformulara su reclamación.

En esta nueva reclamación Schrems afirma que los EE.UU. no ofrecen una protección suficiente de los datos que se transfieren a ese país, y solicita la suspensión o prohibición, de cara al futuro, de las transferencias de sus datos

[25] Decisión de la Comisión de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. [notificada con el número C(2010) 593] (2010/87/UE).

[26] (8) Decisión 2010/87/UE.

[27] Art. 1 de la Decisión 2010/87/UE.

personales desde la UE a los EE.UU. que Facebook Ireland lleva a cabo sobre la base de las cláusulas tipo de protección recogidas en la Decisión 2010/87[28].

Puesta en cuestión la Decisión 2010/87, la autoridad de control irlandesa motivó ante la High Court la necesidad de plantear ante el TJUE una cuestión prejudicial al respecto.

Al tiempo, la UE y los EE.UU. firmaron en 2016 un acuerdo, llamado "Escudo de la privacidad UE-EE.UU.", que venía a sustituir al de puerto seguro, consistente en el ofrecimiento de una serie de garantías por parte de los EE.UU. en materia de protección de los datos personales recibidos por transferencia de un Estado miembro de la UE y que la Comisión Europea venía a considerar adecuadas y, por ende, compatibles con las exigencias de la legislación de la Unión[29].

Afirmaba la Comisión Europea que el Escudo de la privacidad UE-EE.UU. recogía los requisitos establecidos por el TJUE en su sentencia de 6 de octubre de 2015, en la que declaraba inválido el antiguo marco de puerto seguro. El nuevo mecanismo, afirmaba su oficina de prensa, imponía obligaciones más estrictas a las empresas de los EE.UU. y obligaba al Departamento de Comercio de los Estados Unidos y a la Comisión Federal de Comercio (FTC) a un mayor nivel de seguimiento y de ejecución, incluso mediante una mayor cooperación con las autoridades europeas de protección de datos. El nuevo mecanismo incluía compromisos asumidos por los EE.UU. que garantizaban que las posibilidades de acceso de sus autoridades nacionales a los datos personales transferidos en virtud de este mecanismo estarían sujetas a unas limitaciones, condiciones y supervisión claras que impidiesen un acceso generalizado. Así mismo, los europeos tendrían la posibilidad de formular cualquier pregunta o reclamación en este contexto a un nuevo Defensor del Pueblo específico[30].

En la cuestión prejudicial planteada ante el TJUE, el Tribunal Supremo irlandés planteó tres cuestiones básicas: la adecuación al RGPD de las transferencias de datos personales a terceros países basadas en cláusulas tipo de protección y las exigencias de garantía y control que deben incumbir a las autoridades de control nacionales; la validez de la Decisión 2010/87 sobre las cláusulas contractuales tipo; y la validez de la Decisión Escudo de la privacidad[31].

El TJUE en su resolución tomó las siguientes decisiones:

---

[28] Tribunal de Justicia de la Unión Europea. Comunicado de prensa n.º 91/20. Luxemburgo, 16 de julio de 2020. Sentencia en el asunto C-311/18 Data Protection Commissioner/Maximillian Schrems y Facebook Ireland.

[29] 8 Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. (DO 2016, L 207, p. 1).

[30] https://ec.europa.eu/commission/presscorner/detail/es/IP_16_216

[31] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62018CA0311&from=ES

1) declaró que la naturaleza contractual de la Decisión 2010/87 no había de afectar a su validez por el simple hecho de no ser vinculante para las autoridades públicas del tercer país importador de los datos. No obstante, hizo depender esta validez de que la Decisión incluyese mecanismos eficaces que garantizasen, en la práctica, que el nivel de protección exigido por el RGPD fuese respetado y que las transferencias de datos personales basadas en estas cláusulas pudiesen ser suspendidas o prohibidas en caso de su incumplimiento.
2) declaró inválida la Decisión Escudo de la privacidad[32] al afirmar que la legislación estadounidense impone limitaciones a la protección de los datos personales, especialmente con relación a algunos programas que permiten a las autoridades públicas estadounidenses acceder a los datos personales transferidos desde la UE a los EE.UU. con fines de seguridad nacional, de modo que no ofrece unas garantías sustancialmente equivalentes a las que exige el RGPD, y sin que se proporcionase a los titulares de los datos recurso judicial alguno para formular reclamaciones contra las autoridades de los EE.UU.
3) finalmente, en relación al papel que deben desempeñar las autoridades de control nacionales en el contexto de una transferencia de esas características, el Tribunal declaró que, salvo que exista una decisión de adecuación válidamente adoptada por la Comisión, están obligadas a suspender o a prohibir una transferencia de datos personales a un país tercero cuando consideren, a la vista de las circunstancias particulares, que las cláusulas tipo de protección de datos no se respetan o no pueden respetarse en ese país y que la protección de los datos transferidos, en los términos exigidos por el Derecho comunitario, no puede garantizarse mediante otros medios[33].

5. ¿Y tras Schrems I y Schrems II?

Tras la anulación de las Decisiones de puerto seguro y de Escudo de la privacidad, algunos Estados miembros de la UE empezaron a mostrar severa inquietud por las masivas transferencias de datos personales a EE.UU. a través

[32] Decisión 2016/1250 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE- EEUU.

[33] Tribunal de Justicia de la Unión Europea. Comunicado de prensa nº 91/20 Luxemburgo, 16 de julio de 2020. Sentencia en el asunto C-311/18 Data Protection Commissioner/Maximillian Schrems y Facebook Ireland.

del uso extensivo de software propietario y de redes sociales de titularidad de empresas norteamericanas.

A) En Francia

La Conférence des présidents d'université y la Conférence des grandes écoles en 2021 pidieron a la autoridad francesa de control de protección de datos (CNIL) su consideración sobre la compatibilidad de ciertas herramientas de computación en nube de empresas con sede en EE.UU. con las exigencias del RGPD en materia de transferencia internacional de datos.

La invalidación de la Decisión de Escudo de la privacidad por el TJUE generó una enorme preocupación por el uso, en los centros escolares, universitarios y de investigación, de programas como Microsoft Office 365 y Google Workspace que afectaba a una gran cantidad de usuarios, entre estudiantes, investigadores, profesores y personal administrativo, y la capacidad de estas herramientas de procesar una inmensa cantidad de datos, algunos de los cuales podían ser extraordinariamente sensibles (datos de salud, datos de investigación o datos relacionados con menores etc.).

Es más, el ministro francés de educación nacional y juventud, el 30 de agosto de 2022 informó ante la Asamblea Nacional[34] que las versiones gratuitas de Microsoft Office 365 y Google Workspace no debían usarse en las escuelas al considerar que no cumplen las exigencias del RGPD, especialmente desde la sentencia Schrems II, generando un problema de soberanía de datos relacionados con su almacenamiento en un servicio de nube estadounidense[35].

Finalmente, las autoridades francesas determinaron que los servicios en la nube de Microsoft y Google que almacenan datos personales en los EE.UU. no cumplen con la legislación comunitaria ni con las exigencias del TJUE.

Por las mismas razones se puso en entredicho la "Health Data Hub"[36], una infraestructura creada el 30 de noviembre de 2019 con el objetivo de facilitar la centralización y el intercambio de los datos de salud de toda la población tratada en Francia para promover la investigación, y que se puso en servicio de forma anticipada en abril de 2020 para atender la crisis sanitaria del COVID. Se encomendó el alojamiento de la plataforma a Microsoft Azure lo que llevó a diversas asociaciones y profesionales, consecuencia de la sentencia Schrems II, a interponer un recurso ante el Consejo de Estado a fin de solicitar su suspensión.

El Consejo de Estado francés solicitó de la autoridad de control francesa sus observaciones al respecto, manifestando ésta que la elección de un alojamiento sometido al derecho estadounidense era incompatible con las exigencias del TJUE en materia de protección de la privacidad.

[34] https://questions.assemblee-nationale.fr/static/16/questions/jo/jo_anq_202234.pdf
[35] https://www.theregister.com/2022/11/22/france_no_windows_google/
[36] https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub

El Consejo de Estado, a su vez, reconoció el riesgo de que los servicios de inteligencia estadounidenses pudiesen acceder a los datos de salud de los ciudadanos franceses y afirmó el deber de Microsoft de abstenerse de transferir datos de salud a Estados Unidos.

Finalmente, el Secretario de Estado de Asuntos Digitales, el 8 de octubre de 2020 anunció ante el Senado la voluntad del Gobierno de trasladar el Health Data Hub a plataformas francesas o europeas[37].

B) En Alemania

El 22 de septiembre de 2020 la Conferencia de las Autoridades de Protección de Datos alemanas (DSK[38]) sometió a evaluación el programa de Microsoft, Office 365, por la posible infracción requisitos del artículo 28, apartado 3, del RGPD.

Office 365 es un producto propiedad de la empresa tecnológica Microsoft, basado en la nube, y que incluye aplicaciones como Microsoft Teams, Word, Excel, PowerPoint, Outlook y OneDrive. Este producto informático se construye sobre un sistema de código cerrado, también llamado "software propietario", que se caracteriza, en contraposición a los llamados "software libre" o de "código abierto", porque los usuarios desconocen absolutamente el contenido del programa y, por tanto, si existe dentro de las líneas del código de programación alguna amenaza contra su equipo o su información.

Consecuencia de esa evaluación se llegó a la conclusión de que "no era posible utilizar Microsoft Office 365 de forma que cumpliera los requisitos de protección de datos"[39].

En su reunión del 22 de septiembre de 2020, el DSK creó un grupo de trabajo bajo la dirección de Brandenburgo y la Oficina Estatal de Supervisión de Protección de Datos de Baviera (BayLDA) para entablar conversaciones con Microsoft "con el fin de introducir rápidamente mejoras conformes con la protección de datos y a las normas de transferencias a terceros países para la aplicación de la Schrems II"[40].

El informe se cerró el 10 de octubre de 2022 y concluyó que la suite de ofimática Microsoft Office 365 incumple las exigencias del RGPD: almacena datos de menores de edad; permite a Microsoft el acceso a datos no cifrados de los usuarios; transfiere los datos de los usuarios a EEUU, y se reserva el derecho a posibilitar el acceso a los mismos de las autoridades estadounidenses; no se revela plenamente qué operaciones de tratamiento tienen lugar, cuáles se llevan a cabo por cuenta del cliente, ni cuáles se realizan para sus propios fines; no se

[37] https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub
[38] https://www.datenschutzkonferenz-online.de/
[39] https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf
[40] https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

define qué datos personales se tratan para lo que Microsoft denomina fines empresariales "legítimos", o ahora "actividades empresariales"; no revela la base jurídica en que fundamenta la transferencia de los datos personales para su posterior tratamiento para los fines de Microsoft, especialmente datos de telemetría y diagnóstico que Microsoft recopila a gran escala y, fundamentalmente, con fines interesados[41].

En definitiva, el informe concluye que el uso de Microsoft Office 365 resulta inadecuado para su uso en centros escolares y órganos de la administración pública, debido a la falta de transparencia a la hora de recabar datos, su tratamiento, propósitos y fines de este tratamiento, y accesos masivos por las autoridades estadounidenses con infracción del art. 48 del RGPD.

Al tiempo, el DSK recomienda a las empresas y usuarios privados que no utilicen Microsoft 365 dado que no existen garantías de que Microsoft maneje la información recopilada de forma respetuosa con la privacidad.

C) Otros países de la Unión Europea

Las autoridades de protección de datos de Dinamarca y Holanda han puesto en entredicho el cumplimiento por parte de Google de las exigencias del RGPD. Particularmente, las escuelas danesas deben dejar de usar el correo electrónico y los servicios en la nube de Google por violar los estándares de privacidad definidos por el RGPD[42].

6. Hablemos del sistema judicial español

En 2017, el Ministerio de Justicia anunció "en el marco de las actuaciones que se están realizando para realizar la transformación digital de la Justicia", la instalación de Microsoft Office 365 a los jueces, magistrados, fiscales y letrados de la Administración de Justicia[43].

En 2021 el Ministerio de Justicia dotó de licencias de Office 365 a todos los fiscales en todo el territorio español, con posibilidad de acceso al conjunto de herramientas colaborativas y de comunicación de la plataforma Teams[44].

En agosto de 2021, la Dirección General de Transformación Digital de la Administración de Justicia envió una comunicación a las sedes judiciales recomendando el uso del navegador Microsoft Edge para una mejor experiencia con el uso de las aplicaciones de Microsoft 365.

[41] https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

[42]https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag-

[43] Justicia Digital. Nº 18 de 9 de marzo de 2017. ISSN 2530-2019

[44] https://www.fiscal.es/memorias/memoria2022/FISCALIA_SITE/indice.html

En 2021, el Gobierno Vasco encarga a la Sociedad Informática del Gobierno Vasco EJIE, S.A. el diseño e implantación inicial de la solución de Office 365 en la red sectorial de Justicia[45].

En junio de 2022, la Dirección General de Transformación Digital de la Administración de Justicia comunicaba a las sedes judiciales del ámbito territorial competencial del Ministerio de Justicia la actualización del editor de textos del sistema de gestión procesal "Minerva" al paquete Microsoft Office 365 con el propósito de "proporcionar un mayor rendimiento y mejor gestión en la edición y elaboración de los documentos judiciales".

En 2023, el CGPJ ha contratado a una sociedad limitada el suministro de licencias Office 365 y otros productos Microsoft con destino al propio Consejo General del Poder Judicial[46].

En junio de 2023, la Conselleria de Justicia, Interior y Administración Pública de la Generalitat Valenciana anuncia que deja de utilizar la suite ofimática Libre Office y va a iniciar la implantación del software Microsoft 365 en la Administración de Justicia, entre otras. Solicita a todos los órganos judiciales de la Comunidad Valenciana a través de los respectivos correos corporativos, ahora Outlook, la conversión de todos los documentos antiguos generados con Libre Office a las nuevas herramientas corporativas de Microsoft. Se programa el tránsito de software entre junio y diciembre de 2023.

El artículo 236 ter de la LOPJ establece que el tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo, sin perjuicio de las especialidades establecidas en el presente Capítulo y en las leyes procesales.

Este precepto nos conduce al artículo 51 del RGPD que ordena a cada Estado miembro que una o varias autoridades de control asuman la supervisión de la aplicación del Reglamento. En el caso de España esta función se ejerce con carácter general por la Agencia Española de Protección de Datos, excepto para los juzgados y tribunales. Así, el Considerando 20 del RGPD establece que, para preservar la independencia del poder judicial, el control del tratamiento de los datos personales cuando los tribunales actúen en el ejercicio de su función judicial se habrá de encomendar a organismos específicos establecidos dentro del sistema judicial del Estado miembro.

[45] https://www.euskadi.eus/anuncio_contratacion/encargo-sociedad-informatica-del-gobierno-vasco-ejie-s-diseno-e-implantacion-inicial-solucion-office-365-red-sectorial-justicia/web01-tramite/es/

[46] https://contrataciondelestado.es/wps/poc?uri=deeplink:detalle_licitacion&idEvl=An%2BoAAHEdNamq21uxhbaVQ%3D%3D

El artículo 236 octies[47] de la LOPJ se ocupa, entre otras cosas, de determinar las competencias del CGPJ y de la Fiscalía General del Estado como afirmadas autoridades de control respecto de las operaciones de tratamiento efectuadas con fines jurisdiccionales por los Juzgados, Tribunales, Fiscalías y las Oficinas judicial y fiscal.

Por su parte, el artículo 236 nonies se dedica a articular estructuralmente el catálogo competencial del artículo anterior creando una Dirección de Supervisión y Control de Protección de Datos con la que se pretende materializar la nombrada condición del CGPJ como autoridad de control respecto del tratamiento de datos personales que realizan los Juzgados y Tribunales en el ejercicio de sus funciones judiciales.

El RGPD establece en sus artículos 51 a 59 los requisitos, exigencias y garantías que ha de cumplir toda autoridad de control. Así, ha de ser independiente, con recursos propios, materiales, personales y financieros, y, en concreto, que el miembro o los miembros de cada autoridad de control sean ajenos a toda influencia externa, ya sea directa o indirecta, y no soliciten ni admitan ninguna instrucción; ha de disponer en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes; ha de elegir y disponer de su propio personal; y ha de estar sujeta a un control financiero que no afecte a su independencia, disponiendo de un presupuesto anual, público e independiente.

Por su parte, la LOPJ plantea un modelo estructural en el que el CGPJ se presenta como autoridad de protección de datos personales con fines jurisdiccionales, no obstante estar sometido, en el ejercicio de sus competencias en esta materia, a la Agencia Española de Protección de Datos[48] y, al tiempo, deriva el ejercicio de estas atribuidas competencias de control a un órgano cuya jefatura depende del Pleno del propio CGPJ. En definitiva, todo un juego arquitectónico para evitar cumplir los requisitos, exigencias y garantías que impone el RGPD a toda autoridad de control que pretenda serlo.

El resto del artículo orgánico se dedica a recoger algunas de las condiciones que el RGPD dispone para los miembros de las autoridades de control en cuestiones como experiencia y aptitudes técnicas, mandato y régimen de incompatibilidades, y que, sin embargo, la LOPJ atribuye exclusivamente a la persona titular de la Dirección de Supervisión y Control de Protección de Datos, no así al resto del personal que vaya a estar adscrito a la citada Dirección.

Si acudimos a los artículos 53 y 54 del RGPD dedicados a las condiciones generales aplicables a los miembros de la autoridad de control, y a las normas

[47] Según redacción de la Ley Orgánica 7/2021, de 26 de mayo. Ref. BOE-A-2021-8806
[48] Artículo 236 decies de la LOPJ

relativas al establecimiento de la autoridad de control, respectivamente, podemos comprobar que las condiciones de pertenencia, titulación, cualificación y experiencia, cese o destitución en su función, las cualificaciones y condiciones de idoneidad necesarias, los procedimientos para el nombramiento, la duración del mandato, el carácter renovable o no del mandato, las condiciones por las que se rige su ejercicio, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, lo son, todas ellas, para ser nombrado miembro de la autoridad de control, determinar las condiciones de ejercicio de su mandato y hasta su terminación.

Sin embargo, la LOPJ se ocupa, tan solo, de determinar las condiciones del titular de la Dirección de Supervisión. Para el resto de sus miembros, así como para la organización y dirección de esta Dirección de Supervisión, el apartado 6 del artículo comentado ordena que serán objeto de regulación reglamentaria. Y ello a pesar de que los artículos 52 y 54 del RGPD disponen que todas estas condiciones han de ser reguladas por una norma con rango de ley.

Es tal la interdependencia entre el CGPJ y su Dirección de Supervisión que no se deslinda debidamente qué órgano pretende ostentar la cualidad de autoridad de control del sistema judicial. Más bien, todo apunta a que las debilidades estructurales y las dependencias orgánicas del CGPJ en materia de protección de datos personales parecen haber aconsejado derivar las exigencias de la normativa europea en favor de un órgano dependiente reglamentariamente sobre el que construir una suerte de autoridad derivada y con la que salvar una apariencia de regularidad formal.

¿Y el Ministerio Fiscal? El artículo 20.4 del EOMF prevé que en la Fiscalía General del Estado exista una Unidad de Supervisión y Control de Protección de Datos que ejercerá las competencias que corresponden a la autoridad de protección de datos con fines jurisdiccionales sobre el tratamiento de los mismos realizado por el Ministerio Fiscal.

Actualmente no hay constituida en la Fiscalía General del Estado autoridad de control alguna.

7. Y, finalmente, las claves de este viaje (y sus coordenadas)

Iniciábamos este trabajo proponiendo al lector la guía de un viaje: el que realizan los datos de carácter personal desde que son tratados por un tribunal español para los fines propios de su función judicial y hasta su llegada a la retina de algún agente de la inteligencia estadounidense.

A partir de aquí, son varias las coordenadas que localizan los caminos y ubican las sucesivas paradas de ese viaje, estando ya en condiciones de ofrecer los *grados, minutos y segundos* que habrán de servir como sistema de referencia de sus causas, razones e inercias.

Así, hemos de aplicar a este peculiar navegador GPS un Ministerio de Justicia y unas Comunidades Autónomas con las competencias transferidas en materia de justicia que licitan, negocian, contratan y controlan los programas, herramientas y aplicaciones informáticas que se utilizan para gestionar y tramitar los procedimientos judiciales, así como la actividad y comunicaciones de los miembros de los órganos judiciales; una Dirección de Supervisión y Control de Protección de Datos del CGPJ que no es la autoridad de control del sistema judicial porque no cumple las requisitos, exigencias y garantías de los artículos 51 a 59 del RGPD[49]; un CGPJ que tampoco es autoridad de control del sistema judicial porque es un órgano gubernativo sometido a la Agencia Española de Protección de Datos[50]; una AEPD que desde la sentencia del Tribunal Supremo de 2 de diciembre de 2011[51] no es competente para ejercer funciones inspectoras cuando se trata del tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos de los que sean competentes; y una Fiscalía General del Estado que tiene dibujada normativamente[52] una Unidad de Supervisión y Control de Protección de Datos que, se dice, ejercerá las competencias que corresponden a la autoridad de protección de datos con fines jurisdiccionales sobre el tratamiento de los mismos realizado por el Ministerio Fiscal, de acuerdo con lo establecido en el artículo 236 octies de la LOPJ en el ámbito de sus competencias y facultades, y que, sin embargo, sigue sin concreción alguna[53].

En definitiva, invalidada por el TJUE la Decisión Escudo de privacidad, inoperativas las autoridades de control constituidas y silentes las autoridades correspondientes, los datos de carácter personal operados en el sistema judicial español viajan sin control a EE.UU. quedando a disposición, entre otros, de sus agencias de inteligencia.

8. Bibliografía

Comunicación al Parlamento Europeo y al Consejo titulada «Restablecer la confianza en los flujos de datos entre la UE y EE.UU.» [COM(2013) 846 final; en lo sucesivo, «Comunicación COM(2013) 846 final»]

[49] CAPÍTULO VI "Autoridades de control independientes" del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

[50] Art. 236 decies de la LOPJ.

[51] https://web.archive.org/web/20140716040555/http://portaljuridico.lexnova.es/jurisprudencia/JURIDICO/113782/sentencia-ts-sala-3-de-2-de-diciembre-de-2011-agencia-espanola-de-proteccion-de-datos-incompe

[52] Art. 20.4 de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

[53] https://www.fiscal.es/memorias/memoria2022/FISCALIA_SITE/index.html

DECISIÓN DE LA COMISIÓN de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América [notificada con el número C(2000) 2441] (2000/520/CE)

Decisión de la Comisión de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. [notificada con el número C(2010) 593] (2010/87/UE).

Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. (DO 2016, L 207, p. 1).

Petición de decisión prejudicial planteada por la High Court of Ireland (Irlanda) el 25 de julio de 2014—Maximillian Schrems/Data Protection Commissioner (Asunto C-362/14) (2014/C 351/06).

CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2000/C 364/01)

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. (Disposición derogada).

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015. Asunto C-362/14.

Tribunal de Justicia de la Unión Europea. Comunicado de prensa n.º 91/20. Luxemburgo, 16 de julio de 2020. Sentencia en el asunto C-311/18 Data Protection Commissioner/Maximillian Schrems y Facebook Ireland.

Justicia Digital. N.º 18 de 9 de marzo de 2017. ISSN 2530-2019

https://es.wikipedia.org/wiki/Edward_Snowden

https://ec.europa.eu/commission/presscorner/detail/es/IP_16_216

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62018CA0311&from=ES
https://questions.assemblee-nationale.fr/static/16/questions/jo/jo_anq_202234.pdf
https://www.theregister.com/2022/11/22/france_no_windows_google/
https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub
https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub
https://www.datenschutzkonferenz-online.de/
https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf
https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf
https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf
https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag-
https://www.fiscal.es/memorias/memoria2022/FISCALIA_SITE/indice.html
https://www.euskadi.eus/anuncio_contratacion/encargo-sociedad-informatica-del-gobierno-vasco-ejie-s-diseno-e-implantacion-inicial-solucion-office-365-red-sectorial-justicia/web01-tramite/es/
https://contrataciondelestado.es/wps/poc?uri=deeplink:detalle_licitacion&idEvl=An%2BoAAHEdNamq21uxhbaVQ%3D%3D
https://web.archive.org/web/20140716040555/http://portaljuridico.lexnova.es/jurisprudencia/JURIDICO/113782/sentencia-ts-sala-3-de-2-de-diciembre-de-2011-agencia-espanola-de-proteccion-de-datos-incompe
https://www.fiscal.es/memorias/memoria2022/FISCALIA_SITE/index.html

Conflicto de intereses

El autor declara no tener ningún conflicto de intereses.

Financiación

El documento ha sido elaborado sin financiación.